



Person of Non-Interest

[Home \(https://beaponi.com/\)](https://beaponi.com/) > [Learn \(https://beaponi.com/learn\)](https://beaponi.com/learn) > How to turn on two-step verification

How to turn on two-step verification

A second lock on your accounts, so a stolen password isn't enough.

Last reviewed October 18, 2026 · [See the sources](#)

In short: Two-step verification adds a second check after your password, like a code, a tap on your phone, or a security key, so a stolen password alone isn't enough to get in. Turn it on in each account's security settings, starting with your email and bank, and pick the strongest option offered.

What it is

Two-step verification asks for a second proof that it's really you after you enter your password. That might be a code, a tap on your phone, or your fingerprint. If a scammer steals your password, they still can't get in without that second step.

It goes by different names: **two-factor authentication (2FA)**, **multifactor authentication (MFA)**, or **2-Step Verification**. They're often used to mean the same thing: an extra check after your password.

Which kind to choose (best first)

1. **A passkey or security key.** The strongest choice. It can't be typed into a fake website, so it protects you even from convincing scam login pages. What are passkeys? → (<https://beaponi.com/learn/passkeys>)
2. **An authenticator app.** A free app on your phone that shows a new code every 30 seconds.
3. **A code by text message, phone call, or email.** The weakest option, because these codes can be intercepted or tricked out of you. But it's still much better than no second step at all.

Use the strongest option each account offers.

How to turn it on

1. **Open the account's settings.** Look for Settings, Account, or Profile, then Security, or Password and security.
2. **Find two-step verification** under any of the names above and turn it on.
3. **Choose your method,** then follow the prompts to finish.

Save your backup codes. Many accounts give you backup codes when you turn this on. Keep them in your password manager or print them and store them somewhere safe. They get you back in if you lose your phone.

Start with these accounts

- **Your email.** It's the key to resetting everything else.
- **Your bank and payment apps.**
- **Your mobile phone account.** See step 5 of the Starter Checklist (<https://beaponi.com/checklist#doors>) for your carrier's protections.
- **Your Apple or Google account,** and your social media.

Official how-tos: [Turn on 2-Step Verification \(https://support.google.com/accounts/answer/185839\)](https://support.google.com/accounts/answer/185839) (Google) · [Two-factor authentication for Apple Account \(https://support.apple.com/en-us/102660\)](https://support.apple.com/en-us/102660) (Apple)

One rule to never break

Never share a verification code with anyone, even someone who says they're from your bank, Apple, Google, or "support." Real companies don't call to ask for your code. Anyone who asks is trying to get into your account.

A safety note. If you're in an abusive or stalking situation, the other person may notice new security settings. Make a safety plan first. Support is available, for example from the National Domestic Violence Hotline at [thehotline.org \(https://www.thehotline.org\)](https://www.thehotline.org).

Next step

Two-step verification works best with a [strong, unique password \(https://beaponi.com/learn/strong-passwords\)](https://beaponi.com/learn/strong-passwords).

Common questions

Do I need a smartphone for this? Not always. Google, for example, can send a code by text message or phone call to a number you've given it, and also accepts physical security keys. Backup codes you print and keep somewhere safe also work as a second step.

Will I have to enter a code every time I sign in? Not always. Some services, Google for example, let you skip the second step on devices you mark as trusted, like your own computer at home. Don't mark a shared or public computer as trusted.

Should I turn it on for every account? CISA recommends turning it on for every account or app that offers it. If that feels like a lot, start with your email, your bank, and your mobile phone account, and add the rest over time.

Sources

Checked on October 18, 2026. Next review: by October 2027.

- Turn On MFA (<https://www.cisa.gov/secure-our-world/turn-mfa>) (CISA)
- Implementing Phishing-Resistant MFA (<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>) (CISA fact sheet, PDF)
- Digital Identity Guidelines: Authentication, SP 800-63B-4 (<https://pages.nist.gov/800-63-4/sp800-63b.html>) (NIST)
- Turn on 2-Step Verification (<https://support.google.com/accounts/answer/185839>) (Google) · Two-factor authentication for Apple Account (<https://support.apple.com/en-us/102660>) (Apple)

From beaponi.com/learn/two-step-verification · Last reviewed October 18, 2026 · General education, not professional advice.